

CLAIMS

What is claimed is:

1 1. A method of registering a non-configured network device in a telecommunications
2 network, the method comprising the computer-implemented steps of:
3 receiving a message from a first non-configured network device that requests network
4 services;
5 authenticating the first device based on a longer-lived symmetric key received from
6 the first device;
7 generating and providing a shorter-lived symmetric key to the first device based on
8 authenticating the longer-lived symmetric key;
9 receiving a request from a second device to obtain a session key for secure
10 communications between the second device and the first device, based on
11 authenticating the shorter-lived symmetric key, wherein the request includes
12 the shorter-lived symmetric key of the first device;
13 generating and providing a symmetric session key to the second device for use in
14 subsequent secure peer-to-peer communications between the first device and
15 the second device without communication of either the first device or second
16 device to a key management service or authoritative authentication service;
17 and
18 registering the first device in the network.

1 2. A method as recited in Claim 1, wherein the shorter-lived symmetric key is
2 encapsulated in a ticket that includes data identifying a specified lifetime of the shorter-lived
3 symmetric key.

1 3. A method as recited in Claim 1, further comprising the steps of receiving, at the
2 second device, a request from the first device to obtain a session key on behalf of both the
3 first device and second device, wherein the request includes the shorter-lived symmetric key
4 of the first device.

4. A method as recited in Claim 1, wherein the subsequent secure communications comprise successive symmetric encryption and decryption operations using the symmetric session key, and wherein the first device and second device carry out the subsequent secure communications without contact with a key management service or registration service.

5. A method as recited in Claim 1, further comprising the steps of:
receiving a request from a first device that wishes to communicate securely with a second device to register with a trusted registration service;
authenticating the first device; and
in response to authenticating the first device, providing a longer-lived symmetric key to the first device.

6. A method as recited in Claim 1, further comprising the steps of:
authenticating the first device to a trusted registration service; and
in response to authenticating the first device to the trusted registration service, providing the longer-lived symmetric key to the first device.

7. A method as recited in Claim 6, further comprising the steps of:
providing trusted information to the trusted registration service that certifies that the first device as a known device within a security realm; and
providing information identifying the registration service to the first device for use in obtaining the longer-lived symmetric key.

8. A method of distributing cryptographic keys in a network, the method comprising the computer-implemented steps of:
providing a registration service identifier that identifies an administrative entity to a first device and providing a unique identifier of the first device to the administrative entity;

1 12. A method as recited in Claim 9, wherein the step of establishing a longer-lived
 2 symmetric key for the first device comprises the steps of:
 3 generating information that provides assurance to a registration service that the first
 4 device is a certified device; and
 5 authenticating the first device to the registration service by sending a first message
 6 from the first device to the registration service that is encrypted using the
 7 device public key.

1 13. A method as recited in Claim 11, wherein generating information that provides
 2 assurance to a registration service that the first device is a certified device comprises the
 3 steps of creating and storing an association of a unique identifier of the first device and the
 4 device public key in a secure database that is accessible to the registration service, and
 5 providing the unique identifier from the first device to the registration service.

1 14. A method as recited in Claim 9, wherein establishing a longer-lived symmetric key
 2 comprises the steps of:
 3 generating the longer-lived symmetric key;
 4 encrypting the longer-lived symmetric key using the device public key;
 5 encapsulating the encrypted longer-lived symmetric key in a device registration
 6 ticket; and
 7 sending the device registration ticket to the device.

1 15. A method as recited in Claim 14, wherein encapsulating the encrypted key comprises
 2 encapsulating the encrypted longer-lived symmetric key with policy information in the
 3 device registration ticket, wherein the policy information defines a validity interval of the
 4 encrypted longer-lived symmetric key.

16. A method as recited in Claim 8, wherein generating and providing a short-term symmetric key to the first device includes the steps of encapsulating the short-term symmetric key in a short-term ticket granting ticket with associated policy information.

17. A method as recited in Claim 8, wherein the step of receiving a request from a second device to obtain a session key for secure communications among the second device and the first device comprises the steps of:

- receiving a first short-term ticket granting ticket that includes the short-term symmetric key of the first device;
- receiving a second short-term ticket granting ticket that includes the short-term symmetric key of the second device;
- decrypting the first and second short-term ticket granting tickets based on respective first and second shared secret keys;
- authenticating the short-term symmetric keys of the first device and second device based on the respective first and second shared secret keys; and
- generating and providing a symmetric session key to the second device for use in subsequent secure peer-to-peer communications between the first device and the second device without communication of either the first device or second device to a key management service or authoritative authentication service.

18. A method of establishing secure cryptographic peer-to-peer communication between a first device and a second device in a network, the method comprising the computer-implemented steps of:

- providing a unique identifier of the first device and receiving, in response, providing a registration service identifier that identifies an administrative entity to the first device;
- creating and storing a device private key in a secure data repository that is accessible by the administrative entity;
- receiving a longer-lived symmetric key for the first device;

10 authenticating the first device to a key management server using the longer-lived
 11 symmetric key of the first device;
 12 receiving a short-term symmetric key from the key management server, based on
 13 authenticating the longer-lived symmetric key;
 14 generating a request to a second device to obtain a session key for secure
 15 communications among the second device and the first device, based on
 16 authenticating the short-term symmetric key, wherein the request includes the
 17 short-term symmetric key of the first device; and
 18 receiving a symmetric session key from the second device for use in subsequent
 19 secure peer-to-peer communications between the first device and the second
 20 device without communication of either the first device or second device to a
 21 key management service or authoritative authentication service.

1 19. A method as recited in Claim 18, wherein the steps of creating and storing a device
 2 private key with a data repository comprises the steps of generating a public key pair
 3 comprising a device public key and a device private key and storing the device private key in
 4 a database or directory that is accessible to the administrative entity.

1 20. A method as recited in Claim 18, wherein the steps of creating and storing a device
 2 private key with a data repository comprises the steps of generating a public key pair
 3 comprising a device public key and a device private key and registering the device private
 4 key with a certification authority that is accessible to the administrative entity.

1 21. A method as recited in Claim 18, wherein the step of receiving a longer-lived
 2 symmetric key for the first device comprises the steps of:
 3 providing information to a registration service that provides assurance that the first
 4 device is a certified device; and
 5 authenticating the first device to the registration service.

22. A method as recited in Claim 19, wherein the step of receiving a longer-lived symmetric key for the first device comprises the steps of:

- generating information that provides assurance to a registration service that the first device is a certified device; and
- authenticating the first device to the registration service by sending a first message from the first device to the registration service that is encrypted using the device public key.

23. A method as recited in Claim 21, wherein providing information to a registration service that the first device is a certified device comprises the steps of creating and storing an association of a unique identifier of the first device and the device public key in a secure database that is accessible to the registration service, and providing the unique identifier from the first device to the registration service.

24. A method as recited in Claim 19, wherein receiving a longer-lived symmetric key comprises the steps of receiving a device registration ticket that comprises the longer-lived symmetric key encrypted using the device public key.

25. A method as recited in Claim 24, wherein the encrypted longer-lived symmetric key is encapsulated in the device registration ticket with policy information that defines a validity interval of the encrypted longer-lived symmetric key.

26. A method as recited in Claim 18, wherein receiving the short-term symmetric key comprises the steps of receiving the short-term symmetric key in a short-term ticket granting ticket with associated policy information.

27. A method as recited in Claim 18, wherein the step of generating a request from a second device to obtain a session key for secure communications among the second device and the first device comprises the steps of generating a first short-term ticket granting ticket that includes the short-term symmetric key of the first device.

28. A method as recited in Claim 18, wherein the step of receiving a symmetric session key from the second device for use in subsequent secure peer-to-peer communications between the first device and the second device comprises receiving a shared service ticket that contains the symmetric session key.

29. A method as recited in Claim 28, further comprising the steps of:
generating an initial request for peer-to-peer secure communication, wherein the initial request is directed to the second device and includes the shared service ticket;
authenticating the second device based on the symmetric session key in the shared service ticket;
communicating one or more messages to the second device using the symmetric session key to encrypt or decrypt the messages.

30. A computer-readable medium carrying one or more sequences of instructions for distributing cryptographic keys in a network, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:
providing a registration service identifier that identifies an administrative entity to a first device and providing a unique identifier of the first device to the administrative entity;
associating a device private key in a secure data repository that is accessible by the administrative entity;
establishing a longer-lived symmetric key for the first device;
authenticating the first device based on receiving the longer-lived symmetric key from the first device;

generating and providing a short-term symmetric key to the first device based on authenticating the longer-lived symmetric key;
receiving a request from a second device to obtain a session key for secure communications among the second device and the first device, based on authenticating the short-term symmetric key, wherein the request includes the short-term symmetric key of the first device; and
generating and providing a symmetric session key to the second device for use in subsequent secure peer-to-peer communications between the first device and the second device without communication of either the first device or second device to a key management service or authoritative authentication service.

31. An apparatus for distributing cryptographic keys in a network, comprising:
- means for providing a registration service identifier that identifies an administrative entity to a first device and providing a unique identifier of the first device to the administrative entity;
 - means for associating a device private key in a secure data repository that is accessible by the administrative entity;
 - means for establishing a longer-lived symmetric key for the first device;
 - means for authenticating the first device based on receiving the longer-lived symmetric key from the first device;
 - means for generating and providing a short-term symmetric key to the first device based on authenticating the longer-lived symmetric key;
 - means for receiving a request from a second device to obtain a session key for secure communications among the second device and the first device, based on authenticating the short-term symmetric key, wherein the request includes the short-term symmetric key of the first device; and
 - means for generating and providing a symmetric session key to the second device for use in subsequent secure peer-to-peer communications between the first device and the second device without communication of either the first device or second device to a key management service or authoritative authentication service.

- 1 32. An apparatus for distributing cryptographic keys in a data network, comprising:
2 a network interface that is coupled to the data network for receiving one or more
3 packet flows therefrom;
4 a processor;
5 one or more stored sequences of instructions which, when executed by the processor,
6 cause the processor to carry out the steps of:
7 providing a registration service identifier that identifies an administrative
8 entity to a first device and providing a unique identifier of the first
9 device to the administrative entity;
10 associating a device private key in a secure data repository that is accessible
11 by the administrative entity;
12 establishing a longer-lived symmetric key for the first device;
13 authenticating the first device based on receiving the longer-lived symmetric
14 key from the first device;
15 generating and providing a short-term symmetric key to the first device based
16 on authenticating the longer-lived symmetric key;
17 receiving a request from a second device to obtain a session key for secure
18 communications among the second device and the first device, based
19 on authenticating the short-term symmetric key, wherein the request
20 includes the short-term symmetric key of the first device; and
21 generating and providing a symmetric session key to the second device for use
22 in subsequent secure peer-to-peer communications between the first
23 device and the second device without communication of either the first
24 device or second device to a key management service or authoritative
25 authentication.